Adam J Schwartz (SBN 251831)
e-service: adam@ajschwartz.com
ADAM J SCHWARTZ, ATTORNEY AT LAW
5670 Wilshire Blvd., Suite 1800
Los Angeles, CA 90036
phone: (323) 455-4016

Attorney for JOHN BLUMENSTOCK, THOMAS ROSSELLO, and JEFFREY BRANCH and proposed class

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

JOHN BLUMENSTOCK, THOMAS ROSSELLO, and JEFFREY BRANCH on behalf of themselves and all others similarly situated, Plaintiffs, v. ETHOS TECHNOLOGIES, INC., Defendant.	Case No. 3:23-cv-00073 **CLASS ACTION COMPLAINT FOR DAMAGES** **JURY TRIAL DEMANDED**

Plaintiffs, John Blumenstock, Thomas Rossello, and Jeffrey Branch, through their attorneys, bring this Class Action Complaint against the Defendant, Ethos Technologies, Inc. ("Ethos" or "Defendant"), alleging as follows:

INTRODUCTION

1. From August to December 2022, Ethos, an online life insurance company, lost control over thousands of consumers' Social Security numbers during a four-month data breach by cybercriminals ("Data Breach").

2. Ethos' breach differs from typical data breaches because it affects consumers who had no relationship with Ethos, never sought one, and never consented to Ethos collecting and storing their information.

///

3. Ethos sourced their information from third parties, stored it on Ethos' systems, and assumed a duty to protect it, advertising that Ethos "consider[s] safeguarding the security and privacy of customer data an integral part of our mission." But Ethos never implemented the security safeguards needed to fulfill that duty.

4. Indeed, Ethos has suffered two data breaches in less than a year, allowing hackers to exploit the *same* vulnerabilities in its systems twice.

5. The first breach spanned from July 2021 through January 2022, in which hackers bypassed Ethos' cybersecurity to steal consumers' driver's license numbers.

6. They did so by inputting basic information about consumers from public sources on Ethos' website to generate insurance quotes. Hackers could generate a quote with as little as a consumer's name, date, and address.

7. In response, Ethos' system would retrieve information collected from its third-party sources and return a report with expanded information on the consumer, including their driver's license number.

8. Ethos then stored that information in its source code, code Ethos left unprotected and accessible to outsiders like hackers.

9. Using "tools," hackers could then extract consumer information from Ethos' source code.

10. In other words, with basic information on a person's background, hackers could request their driver's license numbers from Ethos and then capture it from Ethos' website—no matter whether the person had a relationship with Ethos, wanted one, or consented to Ethos using their personal information.

11. Ethos learned about the first data breach in January 2022, after hackers had already been farming its systems for consumers' driver's license numbers for five months.

12. Even so, Ethos did not remedy the security vulnerability, leading to an even worse data breach seven months later.

13. In August 2022, hackers used the same method to request quotes and retrieve consumers' *Social Security numbers*.

14. Like the first data breach, Ethos did not detect it when it happened, nor would it for four months.

15. And by the time it did, hackers had already pilfered the personal information belonging to thousands of individuals.

16. The information compromised in this second data breach in August 2022 disclosed consumers' "personally identifiable information" ("PII"), including Social Security numbers, and is the breach at issue in this litigation (the "Data Breach").

17. Plaintiffs are Data Breach victims who had no relationship with Ethos but received its breach notice in December 2022, informing them their Social Security numbers were compromised in the Data Breach. They bring this Class Action on behalf of themselves and all others harmed by Ethos' misconduct in causing its August 2022 Data Breach.

PARTIES

18. Plaintiff, John Blumenstock, is a natural person and citizen of Kentucky, residing in Louisville, Kentucky, where he intends to remain. Mr. Blumenstock is a Data Breach victim, receiving Ethos' Breach Notice in December 2022.

19. Plaintiff, Thomas Rossello, is a natural person and citizen of Florida, residing in Pompano Beach, Florida, where he intends to remain. Mr. Rossello is a Data Breach victim, receiving Ethos' Breach Notice in December 2022.

20. Plaintiff, Jeffrey Branch, is a natural person and citizen of Florida, residing in Naples, Florida, where he intends to remain. Mr. Branch is a Data Breach victim, receiving Ethos' Breach Notice in December 2022.

21. Defendant, Ethos, is a corporation with its principal place of business at 75 Hawthorne Street, Suite 2000, San Francisco, California 94105. It is incorporated in Delaware.

JURISDICTION & VENUE

22. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Ethos.

23. Ethos is incorporated in Delaware and maintains its principal place of business in California at 75 Hawthorne Street, Suite 2000, San Francisco, California 94105. Ethos is thus a Delaware and California citizen.

24. This Court has personal jurisdiction over Ethos because it is a citizen in this District and maintains its headquarters and principal place of business in this District.

25. Venue is proper because Ethos maintains its headquarters and principal place of business in this District.

BACKGROUND FACTS

A. Ethos

26. Ethos is a life insurance company that quotes and sells policies online.

27. As an online company dealing in highly sensitive information, Ethos should understand its duties to safeguard personal information.

28. Indeed, Ethos advertises that securing PII is "an integral part" of its mission:

29. The efforts Ethos claims to have implemented include encryption, multi-factor authentication, and "oversight" from third party security companies.

///

///

///

30. But, on information and belief, Ethos did not implement those security measures as advertised, nor were they reasonably sufficient to protect the highly sensitive data Ethos collected.

31. As Plaintiffs allege above, Ethos collects data on individuals who have no relationship with it, do not want one, and have never consented to its services.

32. It does so by sourcing that information from third parties, "such as private sources (insurance agents, consumer reporting agencies, healthcare providers, health information exchanges, and other data providers)[.]" Those "private sources" supply Ethos data concerning all aspects of consumers' lives, including their health data, familial details, credit scores, location data, "sensory data" on their voices, and "Government-issued identification data," like their driver's license and Social Security numbers.[1]

33. Ethos designed its website to allow anyone with a consumer's basic information to apply for Ethos insurance policies, using as little as their name, address, and birth date.

34. After receiving an application, Ethos retrieves information on the consumer from its third-party sources, then storing it on its website's source code.

35. But despite centering its business model on its website portal, it never secured the highly sensitive information it collects and stores on that portal.

36. As a result, hackers could exploit that vulnerability and steal consumers' information. And they did so twice.

B. Ethos Fails to Safeguard Consumer PII

37. From August 2021 through January 2022, hackers exploited the vulnerability to steal 13,300 consumers' driver's license numbers.

38. Ethos did not detect the hack until January 2022, allowing hackers to pilfer consumers' PII for five months.

39. After detecting the hack, Ethos investigated it and discovered its vulnerability. *See* attached **Exhibit A** for Ethos' breach notice regarding the driver's license number breach.

[1] See Ethos' privacy policy at https://www.ethoslife.com/privacy/ (last accessed January 2, 2023).

40. But even though Ethos discovered the vulnerability and its impact on consumers, Ethos did not fix the problem.

41. Indeed, just seven months later hackers exploited the same vulnerability again, causing an even worse breach.

42. In August 2022, hackers used the same techniques to steal consumers' Social Security numbers.

43. And again, Ethos did not detect the hack when it happened, nor would it for four months.

44. By that time, the damage was done, and hackers had stolen the Social Security numbers belonging to thousands of individuals.

45. Plaintiffs Blumenstock, Rossello, and Branch are individuals and Data Breach victims. They have no relationship with Ethos, never sought one, and never consented to the company using or storing their PII.

46. Even though plaintiffs never had a relationship with Ethos, it still collected their PII and stored it in Ethos' computer systems.

47. In collecting and maintaining the PII, Ethos assumed a duty to safeguard it according to its internal policies and state and federal law.

48. On information and belief, Ethos failed to adequately train its employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over consumer PII twice through the same security vulnerability. Ethos' negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing PII in two data breaches arising from the same problem. Further, Ethos' multiple breach notices make clear that Ethos cannot, or will not, protect the PII it retrieves and possesses on consumers. Attached as **Exhibit B** is a copy of Ethos' second breach notice disclosing the Data Breach affecting consumers' Social Security numbers.

49. Indeed, even Ethos recognizes the threat its Data Breach poses in its breach notice. It offered breach victims credit monitoring and "urged" them to guard themselves against the "potential misuse of information": "we urge you to remain vigilant for incidents of potential

fraud and identity theft, including by regularly reviewing account statements and monitoring your credit reports."

C. Plaintiffs' Experiences

i. Plaintiff Blumenstock.

50. Plaintiff Blumenstock is an individual and data breach victim.

51. Despite never forming or seeking a relationship with Ethos, Plaintiff Blumenstock's PII was compromised in Ethos' second data breach, compromising his Social Security number and exposing him to identity theft and fraud.

52. Indeed, around two weeks after the Data Breach, criminals used his PII to steal $6,800 from his Wells Fargo account.

53. Plaintiff Blumenstock does not recall ever learning that his information was compromised in a data breach incident, other than the breach at issue in this case.

54. As a result of the Data Breach and the recommendations of Defendant's Notice, Plaintiff Blumenstock made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing credit card and financial account statements, changing his online account passwords, placing a credit freeze through the three main credit bureaus, and monitoring his credit information as suggested by Defendant.

55. Indeed, Plaintiff Blumenstok has spent considerable time reaching out to Experian, the designated contact organization for the Ethos Data Breach Response Plan. The information provided by Experian was limited and unable to address Plaintiff Blumenstock's concerns.

56. Plaintiff Blumenstock has spent approximately five hours responding to the Data Breach and will continue to spend valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation.

57. Plaintiff Blumenstock has and will spend considerable time and effort monitoring his accounts to protect himself from identity theft. Plaintiff Blumenstock fears for his personal financial security and uncertainty over what PII was exposed in the Data Breach. Plaintiff Blumenstock has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and

frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

58. Plaintiff Blumenstock is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of unauthorized third parties. This injury was worsened by Defendant's delay in informing Plaintiffs and Class Members about the Data Breach.

59. Plaintiff Blumenstock has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

ii. Plaintiff Rossello

60. Plaintiff Rossello is an individual and data breach victim.

61. Despite never forming or seeking a relationship with Ethos, Plaintiff Rossello's PII was compromised in the Data Breach, compromising his Social Security number and exposing him to identity theft and fraud.

62. Indeed, following the Data Breach, Mr. Rossello suffered identity theft and fraud repeatedly, including the following instances: (i) Bank of America called him to verify a payment card someone tried to open in his name without his authorization; (ii) He received a similar call from JP Morgan Chase seeking to verify a credit card he never opened or authorized; (iii) These instances prompted him to review his credit report, where he saw a hard inquiry from Pentagon Credit Union that he did not authorize. After investigating the inquiry, he learned that someone had tried to open a credit card in his name; and (iv) He learned that criminals had tried to open a credit card in his name 13 times with Check Systems, attempts he never authorized.

63. Given these attempts, Plaintiff Rossello contacted all credit bureaus to freeze his accounts, also contacting his phone provider to lock his phone account. In total, Plaintiff Rossello has devoted 30 hours to remediating the fraud he has suffered.

64. Plaintiff Rosello does not recall ever learning that his information was compromised in a data breach incident, other than the breach at issue in this case.

65. As a result of the Data Breach and the recommendations of Defendant's Notice, Plaintiff Rossello made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing credit card and financial account statements, changing his online account passwords, and monitoring his credit information as suggested by Defendant.

66. Plaintiff Rossello has and will spend considerable time and effort monitoring his accounts to protect himself from identity theft. Plaintiff Rossello fears for his personal financial security and uncertainty over what PII was exposed in the Data Breach. Plaintiff Rossello has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

67. Plaintiff Rossello is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of unauthorized third parties. This injury was worsened by Defendant's delay in informing Plaintiffs and Class Members about the Data Breach.

68. Plaintiff Rossello has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

iii. Plaintiff Branch

69. Plaintiff Branch is an individual and data breach victim.

70. Despite never forming or seeking a relationship with Ethos, Plaintiff Branch's PII was compromised in Ethos' second data breach, compromising his Social Security number and exposing him to identity theft and fraud.

71. Indeed, following the data breach, unauthorized individuals opened two bank accounts in Plaintiff Branch's name at the First National Bank of Omaha, then accessing other accounts belonging to him to transfer around $60,000 from his accounts to fraudulent accounts, a devastating financial loss. As a result, he has spent two days attempting to remediate the harm this identity theft and fraud has caused him.

72. Plaintiff Branch does not recall ever learning that his information was compromised in a data breach incident, other than the breach at issue in this case.

73. As a result of the Data Breach and the recommendations of Defendant's Notice, Plaintiff Branch made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing credit card and financial account statements, changing his online account passwords, and monitoring his credit information as suggested by Defendant.

74. Plaintiff Branch has and will spend considerable time and effort monitoring his accounts to protect himself from identity theft. Plaintiff Branch fears for his personal financial security and uncertainty over what PII was exposed in the Data Breach. Plaintiff Branch has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

75. Plaintiff Branch is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of unauthorized third parties. This injury was worsened by Defendant's delay in informing Plaintiffs and Class Members about the Data Breach.

76. Plaintiff Branch has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

D. Plaintiffs and the Proposed Class Face Significant Risk of Continued Identity Theft

77. Plaintiffs and members of the proposed Class have suffered injury from the misuse of their PII that can be directly traced to Defendant.

78. As a result of Ethos' failure to prevent the Data Breach, Plaintiffs and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PII is used;

b. The diminution in value of their PII;

c. The compromise and continuing publication of their PII;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII; and

h. The continued risk to their PII, which remains in the possession of defendant and is subject to further breaches so long as defendant fails to undertake the appropriate measures to protect the PII in their possession.

79. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained.

80. The value of Plaintiffs' and the proposed Class's PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

81. It can take victims years to spot identity or PII theft, giving criminals plenty of time to use that information for cash.

82. One such example of criminals using PII for profit is the development of "Fullz" packages.

83. Cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of

accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

84. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiffs' and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs' and other members of the proposed Class's stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

85. Defendant disclosed the PII of Plaintiffs and members of the proposed Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII of Plaintiffs and members of the proposed Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII.

86. Defendant's failure to properly notify Plaintiffs and members of the proposed Class of the Data Breach exacerbated Plaintiffs' and members of the proposed Class's injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

E. Defendant failed to adhere to FTC guidelines.

87. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of PII.

///

88. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

89. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

90. The FTC recommends that companies not maintain information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

91. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

92. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers' PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

CLASS ACTION ALLEGATIONS

93. Plaintiffs sues on behalf of themself and the proposed Class ("Class"), defined as follows: "All individuals residing in the United States whose PII was compromised in the Data Breach disclosed by Ethos in December 2022." Excluded from the Class are Defendant, its

agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

94. Plaintiffs reserve the right to amend the class definition.

95. This action satisfies the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

a. **Numerosity**. Plaintiffs are representative of the proposed Class, consisting of thousands of members, far too many to join in a single action;

b. **Ascertainability**. Class members are readily identifiable from information in Defendant's possession, custody, and control;

c. **Typicality**. Plaintiff's claims are typical of Class member's claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

d. **Adequacy**. Plaintiffs will fairly and adequately protect the proposed Class's interests. Their interests do not conflict with Class members' interests, and they have retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

e. **Commonality**. Plaintiffs' and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for all Class members. Indeed, it will be necessary to answer the following questions:

i. Whether Defendant had a duty to use reasonable care in safeguarding Plaintiffs' and the Class's PII;

ii. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

iii. Whether Defendant was negligent in maintaining, protecting, and securing PII;

///

iv. Whether Defendant breached contract promises to safeguard Plaintiffs' and the Class's PII;

v. Whether Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

vi. Whether Defendant's Breach Notice was reasonable;

vii. Whether the Data Breach caused Plaintiffs and the Class injuries;

viii. What the proper damages measure is; and

ix. Whether Plaintiffs and the Class are entitled to damages, treble damages, or injunctive relief.

96. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individual Plaintiffs are insufficient to make individual lawsuits economically feasible.

COUNT I

NEGLIGENCE

(ON BEHALF OF PLAINTIFFS AND THE CLASS)

97. Plaintiffs reallege all previous paragraphs as if fully set forth below.

98. Defendant owed to Plaintiffs and other members of the Class a duty to exercise reasonable care in handling and using the PII in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

99. Defendant owed a duty of care to Plaintiffs and members of the Class because it was foreseeable that Defendant's failure to adequately safeguard their PII in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that PII—just like the Data Breach that ultimately came to pass. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiffs' and members of the Class's PII by disclosing and providing access to this information to third parties and by failing

to properly supervise both the way the PII was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

100. Defendant owed to Plaintiffs and members of the Class a duty to notify them within a reasonable timeframe of any breach to the security of their PII. Defendant also owed a duty to timely and accurately disclose to Plaintiffs and members of the Class the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiffs and members of the Class to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

101. Defendant owed these duties to Plaintiffs and members of the Class because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiffs' and members of the Class's personal information and PII.

102. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that Defendant holds vast amounts of PII, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII—whether by malware or otherwise.

103. PII is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiffs and members of the Class and the importance of exercising reasonable care in handling it.

104. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PII of Plaintiffs and members of the Class which actually and proximately caused the Data Breach and Plaintiffs' and members of the Class's injury. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiffs and members of the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiffs' and members of the Class's injuries-in-fact. As a direct and

traceable result of Defendant's negligence and/or negligent supervision, Plaintiffs and members of the Class have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

105. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiffs and members of the Class actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by criminals, improper disclosure of their PII, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

COUNT II

NEGLIGENCE PER SE

(ON BEHALF OF PLAINTIFFS AND THE CLASS)

106. Plaintiffs and members of the Class incorporate the above allegations as if fully set forth herein.

107. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and members of the Class's PII.

108. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect customers' PII. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiffs' and the members of the Class's sensitive PII.

109. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII Defendant had collected and stored and the foreseeable consequences of a

///

data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

110. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and members of the Class.

111. Defendant had a duty to Plaintiffs and the members of the Class to implement and maintain reasonable security procedures and practices to safeguard Plaintiffs' and the Class's PII.

112. Defendant breached its respective duties to Plaintiffs and members of the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and members of the Class's PII.

113. Defendant's violation of Section 5 of the FTC Act and its failure to comply with applicable laws and regulations constitutes negligence per se.

114. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs and members of the Class, Plaintiffs and members of the Class would not have been injured.

115. The injury and harm suffered by Plaintiffs and members of the Class were the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that Defendant was failing to meet its duties and that its breach would cause Plaintiffs and members of the Class to suffer the foreseeable harms associated with the exposure of their PII.

116. As a direct and proximate result of Defendant's negligence per se, Plaintiffs and members of the Class have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over the value of PII; unreimbursed losses relating to fraudulent charges; losses relating to exceeding credit and debit card limits and balances; harm resulting from damaged credit scores

///

and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen personal information, entitling them to damages in an amount to be proven at trial.

COUNT III

INVASION OF PRIVACY

(ON BEHALF OF PLAINTIFFS AND THE CLASS)

117. Plaintiffs incorporate by reference all preceding allegations.

118. Under California law, a defendant is liable for invasion of privacy if: (1) the plaintiff possessed a legally protected privacy interest, (2) in which the plaintiff maintained a reasonable expectation of privacy, and (3) the defendant's intrusion into that privacy interest was highly offensive. (*See, e.g.*, *Hernandez v. Hillsides, Inc.* (2009) Cal. 4th 272, 287.)

119. Defendant knew, or should have known, that its data security practices were inadequate and had numerous vulnerabilities.

120. Defendant recklessly or negligently failed to take reasonable precautions to ensure its data systems were protected.

121. Defendant knew or should have known that its acts and omissions would likely result in a data breach, which would necessarily cause harm to Plaintiffs and the Class.

122. The exposure of Plaintiffs' information is a highly offensive breach of social norms.

123. Plaintiffs and the Class had a reasonable, legally protected privacy interest in their PII.

124. As a result of Defendant's acts and omissions, third parties accessed the PII of Plaintiffs and the Class without authorization.

125. Defendant is liable to Plaintiffs and the Class for damages in an amount to be determined at trial.

///

///

///

///

COUNT V:

VIOLATIONS OF THE UNFAIR COMPETITION LAW,

BUS. & PROF. CODE § 17200, *ET SEQ.*

(ON BEHALF OF PLAINTIFFS AND THE CLASS)

126. Plaintiffs incorporate by reference all preceding allegations.

127. The California Unfair Competition Law provides that:

> "[U]nfair competition shall mean and include any unlawful, unfair or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising and any act prohibited by Chapter 1 (commencing with Section 17500) of Part 3 of Division 7 of the Business and Professions Code." (BUS. & PROF. CODE § 17200.)

128. Defendant stored the PII of Plaintiffs and the Class in its computer systems and knew or should have known it did not employ reasonable, industry standard, and appropriate security measures that complied with applicable regulations and that would have kept Plaintiffs' and the Class's PII secure and prevented the loss or misuse of that PII.

129. Defendant failed to disclose to Plaintiffs and the Class that their PII was not secure. At no time were Plaintiffs and the Class on notice that their PII was not secure, which Defendant had a duty to disclose.

130. Had Defendant complied with these requirements, Plaintiffs and the Class would not have suffered the damages related to the data breach.

131. Defendant's conduct was unlawful, in that it violated the policy set forth in California's Consumer Records Act, requiring the safeguard of personal information like Social Security numbers, the FTCA, as identified above, and Defendant's common law duty to safeguard PII.

132. Defendant's conduct was also unfair, in that it violated a clear legislative policy in favor of protecting consumers from data breaches.

133. Defendant also engaged in unfair business practices under the "tethering test." Its actions and omissions, as described above, violated fundamental public policies expressed by the

California Legislature. *See, e.g.*, Cal. Civ. Code § 1798.1 ("The Legislature declares that . . . all individuals have a right of privacy in information pertaining to them . . . The increasing use of computers . . . has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information."); Cal. Civ. Code § 1798.81.5(a) ("It is the intent of the Legislature to ensure that personal information about California residents is protected."); Cal. Bus. & Prof. Code § 22578 ("It is the intent of the Legislature that this chapter [including the Online Privacy Protection Act] is a matter of statewide concern."). Defendant's acts and omissions thus amount to a violation of the law.

134. As a result of those unlawful and unfair business practices, Plaintiffs and the Class suffered an injury-in-fact and have lost money or property.

135. The injuries to Plaintiffs and the Class greatly outweigh any alleged countervailing benefit to consumers or competition under all of the circumstances.

136. There were reasonably available alternatives to further Defendant's legitimate business interests, other than the misconduct alleged in this complaint.

137. Therefore, Plaintiffs and the Class are entitled to equitable relief, including restitution of all monies paid to or received by Defendant; disgorgement of all profits accruing to Defendant because of its unfair and improper business practices; a permanent injunction enjoining Defendant's unlawful and unfair business activities; and any other equitable relief the Court deems proper.

COUNT V

DECLARATORY JUDGMENT AND INJUNCTIVE RELIEF

(ON BEHALF OF PLAINTIFFS AND THE CLASSES)

138. Plaintiffs incorporate all previous paragraphs as if fully set forth below.

139. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as those alleged herein, which are tortious and which violate the terms of the federal and state statutes described above.

140. An actual controversy has arisen in the wake of the Data Breach at issue regarding Defendant's common law and other duties to act reasonably with respect to employing reasonable data security. Plaintiffs allege Defendant's actions in this respect were inadequate and unreasonable and, upon information and belief, remain inadequate and unreasonable. Additionally, Plaintiffs and the Classes continue to suffer injury due to the continued and ongoing threat of new or additional fraud against them or on their accounts using the stolen data.

141. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owed, and continues to owe, a legal duty to employ reasonable data security to secure the PII it possesses, and to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTC Act;

b. Defendant breached, and continues to breach, its duty by failing to employ reasonable measures to secure its customers' personal and financial information; and

c. Defendant's breach of its legal duty continues to cause harm to Plaintiffs and the Classes.

142. The Court should also issue corresponding injunctive relief requiring Defendant to employ adequate security protocols consistent with industry standards to protect its employees' (i.e. Plaintiffs and the Classes') data.

143. If an injunction is not issued, Plaintiffs and the Classes will suffer irreparable injury and lack an adequate legal remedy in the event of another breach of Defendant's data systems. If another breach of Defendant's data systems occurs, Plaintiffs and the Classes will not have an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages, while warranted to compensate Plaintiffs and the Classes for their out-of-pocket and other damages that are legally quantifiable and provable, do not cover the full extent of injuries suffered by Plaintiffs and the Classes, which include monetary damages that are not legally quantifiable or provable.

144. The hardship to Plaintiffs and the Classes if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued.

145. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach, thus eliminating the injuries that would result to Plaintiffs, the Classes, and the public at large.

PRAYER FOR RELIEF

146. Plaintiffs and members of the Class demand a jury trial on all claims so triable and request that the Court enter an order:

a. Certifying this case as a class action on behalf of Plaintiffs and the proposed Class, appointing Plaintiffs as class representative, and appointing their counsel to represent the Class;

b. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiffs and the Class;

c. Awarding injunctive relief as is necessary to protect the interests of Plaintiffs and the Class;

d. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen PII;

e. Awarding Plaintiffs and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

f. Awarding restitution and damages to Plaintiffs and the Class in an amount to be determined at trial;

g. Awarding attorneys' fees and costs, as allowed by law;

h. Awarding prejudgment and post-judgment interest, as provided by law;

i. Granting Plaintiffs and the Class leave to amend this complaint to conform to the evidence produced at trial; and

j. Granting such other or further relief as may be appropriate under the circumstances.

///

JURY DEMAND

147. Plaintiffs demands a trial by jury on all issues so triable.

Respectfully Submitted
ADAM J SCHWARTZ ATTORNEY AT LAW

Dated: January 6, 2023

by: _____
Adam J Schwartz

Attorney for JOHN BLUMENSTOCK, THOMAS ROSSELLO, and JEFFREY BRANCH and proposed class